CLAIMS

1. A method of preventing intrusion in communication traffic with a set (130) of machines in a network, said traffic comprising communication entities, the method including the steps of:

- providing a test system (420) including test facilities (421) replicating at least one of said machines in said set (130),

- directing at least part of said communication entities in said traffic towards said test system (420),

- running said communication entities directed towards said test system (420) on said test facilities (421) to detect possibly adverse effects on said test system (420), and

- i) in the presence of an adverse effect, blocking the communication entities leading to said adverse effect, and

- ii) in the absence of an adverse effect, allowing communication with said set (130) of machines for the communication entities failing to lead to said adverse effect.

2. The method of claim 1, characterized in that said at least part of said communication entities directed towards said test system (420) include communication entities from traffic bound towards said set (130) of machines.

3. The method of claim 1, characterized in that said at least part of said communication entities directed towards said test system (420) include communication entities from traffic coming from said set (130) of machines.

4. The method of claim 1, characterized in that it includes the steps of:

- providing a data base (415) including patterns representative of forbidden communication entities for communication with said set of machines (130),

- blocking (412a) forbidden communication entities in said traffic as identified by respective patterns included in said data base (415).

5. The method of claim 1, characterized in that it includes the steps of:

- providing a further data base (416) including patterns representative of allowed communication entities for communication with said set of machines (130),

- allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base (416).

6. The method of claim 4, characterized in that it includes the steps of:

- detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base (415), and

- directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base (415) towards said test system (420) to be run on said test facilities (421) to detect possibly adverse effects of on said test system (420).

7. The method of claim 6, characterized in that it includes, in the presence of said adverse effect, the step of adding to said data base (415) the respective pattern identifying the communication entity leading to said adverse effect.

8. The method of claim 5, characterized in that it includes the steps of:

- detecting unknown communication entities in said traffic as identified by respective unknown pattern not included in said further data base (416), and

- directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said further data base (416) towards said test system (420) to be run on said test facilities (421) to detect possibly adverse effects of on said test system (420).

9. The method of claim 8, characterized in that it includes, in the absence of said adverse effect, the step of adding to said further data base (416) the respective pattern identifying the communication entity failing to lead to said adverse effect.

10. The method of claim 1, characterized in that it includes, in the presence of said adverse effect, the step of subjecting to a resetting step those of said test facilities (421) in said test system (420) affected by said adverse effect.

11. The method of claim 1, characterized in that, the machines in said set (130) including facilities exposed to said adverse effect as well as additional contents, it includes the step of configuring said test facilities (421) in order to replicate said facilities exposed to said adverse effect in the machines in said set (130).

12. The method of claim 1, characterized in that it includes the step of inhibiting said test machines (421) in said test system (420) from providing responses to said traffic.

13. The method of claim 1, characterized in that it includes the steps of:

- providing an in-line component (410) ensuring said traffic with said set of machines (130), and

- providing at least one interface (411d) interfacing said in-line component (410) with said test system (420).

14. The method of claim 13, characterized in that it includes the step of providing feedback from said test system (420) to said in-line component (410) via said at least one interface (411d).

15. The method of claim 13, characterized in that it includes the steps of:

- providing a management network (414) for managing said test system (420), and

- providing feedback from said test system (420) to said in-line component (410) via said management network.

16. The method of claim 7, characterized in that it includes the steps of:

- providing a parallel intrusion preventing arrangement including a respective data base including patterns representative of respective forbidden communication entities for communication with a respective set of machines,

- in the presence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective data base, the respective pattern identifying the communication entity leading to said adverse effect.

17. The method of claim 9, characterized in that it includes the steps of:

- providing a parallel intrusion preventing arrangement including a respective further data base including patterns representative of respective allowed communication entities for communication with a respective set of machines,

- in the absence of said adverse effect, transmitting to said parallel intrusion preventing

arrangement, for inclusion in said respective further data base, the respective pattern identifying the communication entity failing to lead to said adverse effect.

18. A system of preventing intrusion in communication traffic with a set (130) of machines in a network, said traffic comprising communication entities, the system including:

- a test system (420) including test facilities (421) replicating at least one of said machines in said set (130),

- a communication module (410) configured for directing at least part of said communication entities in said traffic towards said test system (420), wherein said communication entities directed towards said test system (420) are adapted to be run on said test facilities (421) to detect possibly adverse effects on said test system (420),

said communication module (410) being further configured for

- i) in the presence of an adverse effect, blocking the communication entities leading to said adverse effect, and

- ii) in the absence of an adverse effect, allowing communication with said set (130) of machines for the communication entities failing to lead to said adverse effect.

19. The system of claim 18, characterized in that said communication module (410) is configured for including in said at least part of communication entities directed towards said test system (420) communication entities from traffic bound towards said set (130) of machines.

20. The system of claim 18, characterized in that said communication module (410) is configured for

including in said at least part of communication entities directed towards said test system (420) communication entities from traffic coming from said set (130) of machines.

21. The system of claim 18, characterized in that it includes:

- a data base (415) including patterns representative of forbidden communication entities for communication with said set of machines (130),
- a firewall module (412a) configured for blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base (415).

22. The system of claim 18, characterized in that it includes:

- a further data base (416) including patterns representative of allowed communication entities for communication with said set of machines (130),
- said communication module (410) configured for allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base (416).

23. The system of claim 21, characterized in that said communication module (410) is configured for:

- detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base (415), and
- directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base (415) towards said test system (420) to be run on said test facilities (421) to detect possibly adverse effects of on said test system (420).

24. The system of claim 23, characterized in that said communication module (410) is configured for

adding to said data base (415), in the presence of said adverse effect, the respective pattern identifying the communication entity leading to said adverse effect.

25. The system of claim 22, characterized in that said communication module (410) is configured for:

- detecting unknown communication entities in said traffic as identified by respective unknown pattern not included in said further data base (416), and

- directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said further data base (416) towards said test system (420) to be run on said test facilities (421) to detect possibly adverse effects of on said test system (420).

26. The system of claim 25, characterized in that said communication module (410) is configured for adding to said further data base (416), in the absence of said adverse effect, the respective pattern identifying the communication entity failing to lead to said adverse effect.

27. The system of claim 18, characterized in that said test facilities (421) in said test system (420) are configured to undergo resetting following said adverse effect.

28. The system of claim 18, characterized in that the machines in said set (130) include facilities exposed to said adverse effect as well as additional contents, while said test facilities (421) replicate said facilities exposed to said adverse effect in the machines in said set (130).

29. The system of claim 18, characterized in that the test machines (421) in said test system (420) are inhibited from providing responses to said traffic.

30. The system of claim 18, characterized in that it includes:

- an in-line component in said communication module (410) ensuring said traffic with said set of machines (130), and

- at least one interface (411d) interfacing said in-line component (410) with said test system (420).

31. The system of claim 30, characterized in that said test system (420) is configured for providing feedback to said in-line component (410) via said at least one interface (411d).

32. The system of claim 30, characterized in that it includes a management network (414) for managing said test system (420) and in that said test system (420) is configured for providing feedback to said in-line component (410) via said management network.

33. The system of claim 24, characterized in that it includes an associated parallel intrusion preventing arrangement including a respective data base including patterns representative of respective forbidden communication entities for communication with a respective set of machines and in that said communication module (410) is configured for transmitting, in the presence of said adverse effect, to said parallel intrusion preventing arrangement, for inclusion in said respective data base, the respective pattern identifying the communication entity leading to said adverse effect.

34. The system of claim 25, characterized in that it includes an associated parallel intrusion preventing arrangement including a respective further data base including patterns representative of respective allowed communication entities for communication with a respective set of machines and in that said communication module (410) is configured for transmitting, in the absence of said adverse effect, said parallel intrusion preventing arrangement, for

inclusion in said respective further data base, the respective pattern identifying the communication entity failing to lead to said adverse effect.

35. A telecommunication network (110, 130) including the system of any of claims 18 to 34.

36. A computer program product loadable in the memory of at least one computer and including software portions for performing the steps of the method of any of claims 1 to 17.